ABSTRACT

This invention proposes a method for securing updating software in a plurality of decoders based on the generation of a signature by means of a private asymmetrical key. The updating of a decoder is carried out by downloading, from a managing center, a data block including a patch and its signature, said block is stored in a RAM. The signature is decrypted with a current public key from a list contained in a first non-volatile memory of the decoder, then verified and in the case of correspondence, a command leads the installation of the patch in a second non-volatile Flash memory and the deactivation of the current key. The aim of this invention is to considerably reduce the impact of the discovery of a private key by mean of a systematic analysis of the working of the decoder software, or to notably increase the time and the means necessary for the process used to determine said private key.